# Rules of Behavior for Information System Security Officers

## A Mandatory Reference for ADS Chapter 545

New Reference:  06/01/2006
Responsible Office:  M/DCIO
File Name:  545mbb_060106_cd44

# Information System Security
# Rules of Behavior
## for Information System Security Officers

## Table of Contents

## Information Systems Security User Rules of Behavior

### 1. Rules of Behavior Overview

Within ADS 545, five NIST-defined roles have corresponding rules of behavior (ROBs). These five roles are User, System Administrator, Information System Security Officer (ISSO), Functional Management, and Executive Management. User rules of behavior apply to all USAID personnel who use information systems. The other four roles have rules of behavior that are specific to their classification alone, and that will take precedence over the rules of behavior defined for the User role.

### 2. User Responsibilities

Users are individuals who are authorized by privilege to use information system and networks. A user can also be an individual who uses information processed by any information system.

### 3. User Rules of Behavior

This section contains the Rules of Behavior (ROB) as derived from the policies contained in **ADS 545, Information System Security Policy**.

This set of ROB supplements the User ROB. The rules contained in this document take precedence over the User ROB when there is a conflict with specific rules. If you have questions about the ROB, please contact your local ISSO or CISO's office.

You must sign and return an acknowledgement for each copy of the ROB that you are responsible for based upon your role(s). The acknowledgement page(s) indicates that you have received, read, and that you understand your responsibilities as a user of USAID General Support System information systems. You further agree to follow the rules of behavior and understand that you may be subject to the penalties specified in ADS 545 for infractions of the rules of behavior.

The ROB may reference other documents such as policy, standards, procedures, guidelines or other related items.

### 3.1 Broad Organizational Rules of Behavior

**a.** Information System Security Officers, System Administrators, and other privileged users must not test, bypass, modify, or deactivate security controls used to protect USAID's information systems, unless authorized in writing to do so by the CISO.

**b.** The General Support System (GSS) ISSO must specify the points of control for Agency computing and telephony resources.

### 3.1.1 Information Assurance

You must establish and maintain procedures for conducting certifications and accreditations, annual security reviews, and system testing and evaluations.

### 3.1.2 Incident Handling

You, the CISO, GSS ISSO, and System ISSOs must train staff to recognize and respond to security incidents.

The USAID basic incident handling procedures, developed by the CISO, to comply with the US-CERT processes, are contained in **Incident Identification and Reporting Procedures**.

### 3.1.3 User Support

The following policies state that USAID must establish a user support capability to generate an initial response and react to a reported security incident.

**a.** You, the Help Desk, System Administrators, or information security staff must follow incident reporting procedures, developed and documented by the CISO, the GSS Security Operations Staff, and System ISSOs, and must act immediately if a security incident is reported.

**b.** You, the Help Desk or System Administrators must document all reported security incidents, as specified in the USAID basic or system-specific incident reporting procedures.

**c.** You and System Owners must document information system-specific help desk and incident handling procedures in their information systems' System Security Plans.

### 3.1.4 General Software Support

You and System Owners must implement security controls on their information systems, or use a capability provided by the CISO or the GSS ISSO, to detect changes to software on each system.

USAID stated virus detection guidelines are contained in **Virus Detection Guidelines**.

### 3.1.5 Software Maintenance

You and System Administrators, with CISO approval, may use hardware or software for testing information system vulnerabilities.

### 3.1.6 Physical Facilities and Restricted Spaces

One or more of Office of Security (SEC), the CISO, the GSS ISSO, or the System ISSO must approve facilities that are located in the continental United States and that contain USAID information systems or house USAID staff.

Physical facilities and restricted spaces security procedures are contained in **Restricted Access Procedures and Guidelines**.

### 3.1.7 Networks and Workstation Connectivity

The following policies govern network and workstation connectivity, i.e., the interlinking of computers across one or more physical sites. Management must take steps to keep the network and its devices secure from outside intruders.

**a. Networks**

1. ISSOs, System Administrators and other privileged users must not use network monitoring and testing equipment unless authorized to do so by the CISO.

2. Staff must not publicly release any information about USAID networks without the approval of the CISO, the GSS ISSO, or their System ISSO.

**b. Firewalls**

1. The GSS ISSO must approve the use of firewalls and all changes to them, using CISO approved procedures.

2. System Administrators must validate new firewall configurations, and the GSS ISSO and the IRM CCB must approve the new configuration before production deployment.

3. System Administrators and the GSS ISSO must evaluate and approve all new firewalls and new connectivity paths for security risks.

4. System Administrators and the GSS ISSO must periodically review firewall logs to check for anomalies.

### c. Production & Development Servers

1. The System ISSO must approve all significant changes to production servers.

2. System Administrators and the System ISSO must evaluate all new servers and their interconnections for security risks.

The wireless access standards are contained in **Wireless Access Standards and Guidelines**.